Amendments to the Specification:

Please replace paragraph **[22]** with the following amended paragraph:

[22] Figs. 4B-4G are example Web pages generated by IP data processing system 100 that are accessible to a client system through the home Web page shown in Fig. 4A according to one embodiment of the present invention[[; and]]

Please replace paragraph **[23]** with the following amended paragraph:

[23] Fig. 5 is a simplified block diagram of an intellectual property data processing system 200 according to a second embodiment of the present invention;[[.]]

Please add the following new paragraphs after paragraph **[23]**:

[23A] Fig. 6 shows an embodiment of a group hierarchy according to the present invention;

[23B] Fig. 7 shows an example of hierarchy of groups according to an embodiment of the present invention;

[23C] Fig. 9 is a simplified high-level flowchart depicting a method of a data access technique for the documents of a Case Data Unit according to an embodiment of the present invention that includes roles and permissions, groups, and Case Data Unit level access information; and

[23D] Fig. 10 is a simplified high-level flowchart depicting a method of a data access technique for a private folder and its associated documents according to an embodiment of the present invention that includes groups.

Please replace paragraph **[45]** with the following amended paragraph:

[45] One benefit of IP data processing system 100 is the way information is assembled and managed. In some embodiments, system 100 acts as a central data repository of all information that is relevant to the patent process. Such data and information is stored by system

100 in database 106 and managed using Case Data Units, where each Case Data Unit is a collection of data and/or documents that are related to a particular case, e.g., a patent application in a particular country. In some instances a case may actually include more than one patent application, for example, where a Continued Prosecution Application (CPA) is filed in the USPTO under rule 37 C.F.R. 1.53(d). The Case Data Unit may be implemented as a data structure, a file, a database, or any other structure capable of storing data and/or documents and provides the logical centralization of data.

Please replace paragraph **[49]** with the following amended paragraph:

[49] As stated above, access management system 109 provides security services for the patent-related information in system 100. As can be seen from Fig. 2, several entities may need to access data stored in a Case Data Unit for a particular case. ~~According to an embodiment of the invention, the access management system is a gateway, either allowing or disallowing various operations to be performed upon data and/or documents associated with a case. According to one embodiment, access management system 109 either allows or disallows users to perform operations upon a Case Data Unit according to rules and permissions assigned to a user, as well as group assignment of both users and Case Data Units. Other embodiments of the access management system further provide Case Data Unit level access information.~~

Please add the following new paragraphs after paragraph **[49]**:

[49A] For example, where a company uses the present invention to manage its patent portfolio, the company will have persons of different levels throughout the organization that may need access to Case Data Unit data for a particular patent application or file. These persons may include persons in the legal department who maintain the file, one or more inventor(s) who created or drafted the invention disclosure(s), the patent coordinator for the business unit that makes the decision on whether or not to file the invention, and others. Further, the degree of access to the Case Data Unit is not the same for each of these persons. For example, a company's would allow an inventor access to disclosures but would not want the inventor to have access to an application. Further, a company's patent coordinator may have access to correspondences with an outside law firm that is prosecuting a case but the patent coordinator would not have access to an application. Other examples for which the degree of access to the

case data may be restricted to a limited number of users include a company's files which are in the process of negotiations such that only persons with a need to know should have access to the file (to prevent inappropriate information dissemination which may expose the company to liabilities e.g., insider trading).

[49B] If a company uses an outside law firm to handle one or more cases, the company may want to grant the law firm personal access to the Case Data Units. However, within the law firm there may be persons who for an ethical reason may not to have access to the Case Data Unit data (e.g., because a person worked for a competitor or for a party adverse to the company).

[49C] According to an embodiment of the invention, the access management system is a gateway, either allowing or disallowing various operations to be performed upon data and/or documents associated with a case. According to one embodiment, access management system 109 either allows or disallows users to perform operations upon a Case Data Unit according to rules and permissions assigned to a user, as well as group assignments of both users and Case Data Units. Other embodiments of the access management system further provide access control techniques associated with each individual Case Data Unit level access information. Each of these data access control techniques are described below in further detail. It should be apparent that in alternative embodiments of the present invention, other data access control techniques may also be used.

Please replace paragraph **[50]** with the following amended paragraph:

[50] Access management system 109 assigns users (client systems) of system 100 and Case Data Units to one or more groups. ~~A user assigned to a group will have access to the Case Data Units in that group and any subsets of the group. Similarly, users not assigned to the group will not have access to Case Data Units in that group.~~ Examples of specific groups may include: Company X, Division M of Company X, Division of N of Company X, law firm Y, client team R in law firm Y, or any other logical groupings of related client systems.

Please add the following <u>new</u> paragraphs after paragraph **[50]**:

[50A] According to one embodiment, data access techniques include the utilization of group hierarchies and the assignment of cases and users to groups within the hierarchy.

According to an embodiment, a user will have access to a Case Data Unit if the user and Case Data Unit are assigned to the same group. According to another embodiment, a user will have access to a Case Data Unit if the user's assigned group contains the group to which the Case Data Unit is assigned. The groups to which users and cases are assigned may be structured hierarchically. Group assignment is discussed in further detail below.

[50B] Various group hierarchies can be implemented to control user access to Case Data Units. Fig. 6 shows a group hierarchy 300 according to an embodiment of the present invention. Group 310 of the hierarchy is said to contain groups 315 and 320. Further, group 315 is said to contain and groups 325, 330, and 335. Further, group 315 is said to contain groups 325, 330, and 335. Thus, group 310 can be considered to contain groups 325, 330, and 335. Cases may be assigned to a group (e.g., group 335) or a set of groups (e.g., groups 325 and 330). For example, while case 365 is assigned to group 325, case 370 is assigned to both groups 325 and 330. However, case 370 need not be assigned to group 335. Thus, if a user is assigned to group 335 and not to groups 310, 315, 325, or 330, the user will not be allowed access to case 370 and accordingly will not be allowed to perform operations on the Case Data Unit associated with case 370. Also, cases may be assigned to a group (e.g., group 310) that contains other groups (e.g., 315 and 320). If a case is assigned to a group that contains other groups, the case is said to be assigned to both the group containing the other groups and to the contained groups. For example, Case Data Unit 350 assigned to group 310 is said to be assigned to groups 315 and 320 contained by group 310.

[50C] According to another embodiment of the invention, a group hierarchy may include two sets of groups. For convenience the two sets of groups are referred to as a first set of group and a second set of groups. A group of the first set of groups may or may not contain one or more groups of the second set of groups. According to one embodiment, cases may be assigned to either groups of the first or second set of groups. According to another embodiment cases may be assigned to groups of the second set of groups but are not assigned to groups of the first set of groups. Fig. 7 shows an example of a hierarchy of groups 400 having Case Data Units assigned to groups 415, 420, and 425. Groups 415, 420, and 425 are said to be of a second set while group 410 is said to be of a first set. According to another embodiment groups are not in a hierarchy but are limited to groups that do not contain other groups.

[50D] Each of these hierarchies of groups may similarly be described in terms of levels while describing the same functionality as that discussed above. For example, a so-called level zero groups would contain subgroups but would not be contained by other groups. Further, each level of group containment by another group can be labeled/described by the number of groups it is contained by. In the example of Fig. 6, group 310 would be a level zero group, groups 315 and 320 would be level one groups, and groups 325, 330, and 335 would be level two groups. Those of skill in the art will undoubtedly know of other useful group hierarchy and further useful ways of describing such hierarchies.

[50E] A user assigned to a group will have access to the Case Data Units in that group and any subsets of the group. Similarly, users not assigned to the group will not have access to Case Data Units in that group.

[50F] For example, Fig. 6 shows a user 390 assigned to group 325. Moreover, Case Data Units 365 and 370 belong to the group 325. As user 390 and Case Data Units 365 and 370 belong to the group 325, accordingly user 390 will have access to these Case Data Unit 365 and 370. According to a further example, Fig. 3 shows user 395 assigned to group 315. Group 315 contains the groups 325, 330, and 335. Case 365 having a Case Data Unit is assigned to group 365. As user 395 is assigned to a group 315 that contains group 325, accordingly user 395 will have access to the Case Data Units belonging to group 325. According to a further example, Fig. 6 shows user 397 assigned to group 320. As group 320 has not been assigned case 365 and its associated Case Data Unit and as group 320 does not contain a group that contains case 365, accordingly user 397 will not have access to case 365 and its associated Case Data Unit.

Please replace paragraph **[53]** with the following amended paragraph:

[53] Roles, in turn, have default sets of documents types assigned to them. The assignment of a given document type to a given role allows a user assigned the given role to make certain manipulations upon documents of that type. <u>As described above, a Case Data Unit may store one or more electronic documents (or references to one or more electronic documents) related to a particular case. Each document may be classified as belonging to a particular type.</u> Specific examples of document types include an invention disclosure, a filed patent application, patent drawings, old versions of patent applications and drawings, other patent papers (e.g., other

documents filed in the patent office including: responses to office actions, information disclosure statements, petitions, etc.); forms, image files (e.g., locked documents of .pdf or a similar type of image file format corresponding to a granted patent (if a patent was granted for the case) as well as image file format copies of any office actions received, responses filed in the patent office, filing receipts, etc. issued during prosecution of the patent application); notes (e.g., practitioner notes, inventor notes, notes from other interested parties regarding the importance of the patent to a company's business, products or competitor's business or products, etc.); mail (e.g., email messages or alerts) and prior art references among others.

Please replace paragraph **[54]** with the following amended paragraph:

[54] Finally, access to Case Data Units can be granted or denied on an individual case level. For example, a Case Data Unit level access can be used to deny, for conflict purposes (e.g., an ethical wall), an individual client system access to a Case Data Unit sharing a common group assignment with the client system. ~~Further details of the use of roles, permissions, groups and Case Data Units according to one embodiment of the invention are set forth in concurrently filed U.S. Provisional Application Number 60/333,962 entitled "DATA ACCESS CONTROL TECHNIQUES USING ROLES AND PERMISSIONS" and having Stephen K. Boyer, Jeffry J. Grainger and Cecily Anne Snyder as inventors. The 60/333,962 application is hereby incorporated by reference in its entirety.~~

Please add the following <u>new</u> paragraphs after paragraph **[54]**:

[54A] According to one embodiment of the invention, each Case Data Unit has unique Case Data Unit level access information. Case Data Unit level access information provides that regardless of group assignment, a user can be granted or denied access to a Case Data Unit and/or its associated documents. The Case Data Unit level access information for each Case Data Unit is comprised of an include list and an exclude list. If a user is entered onto the include list for the Case Data Unit level access information of a given Case Data Unit the user is given access to the Case Data Unit and may perform operations upon Case Data Unit and is associated document determinant upon the user's assigned permissions. If however a user is entered onto the exclude list the Case Data Unit level access information of a given Case Data Unit the user is denied access to the Case Data Unit and is associated document. Thus, regardless of whether a

user and a Case Data Unit are not assigned to the same group and regardless of whether a user's assigned group does not contain the group to which the Case Data Unit is assigned, the include list of the Case Data Unit level access information overrides the exclusion based on group assignment. And further, regardless of whether a user and the Case Data Unit are assigned to the same group and regardless of whether a user's assigned group contains the group to which the Case Data Unit is assigned, the exclude list of the Case Data Unit level access information overrides the access based on group assignment.

[54B] According to one embodiment of the present invention, a user may neither be placed on the include list nor exclude list for the Case Data Unit level access information of a given Case Data Unit. In such a condition, whether a user can perform operations upon a Case Data Unit is determined upon whether the user and Case Data Unit are assigned to the same group or whether the user's assigned group contains the group to which the Case Data Unit is assigned, (described in detail above).

[54C] According to another embodiment of the present invention, users can be automatically added to an include or exclude list based upon their role assignment or other rules. Rules may include a combination of logical expressions that either indicate the automatic placement of a user on an include or exclude list. Logical expressions may include compound logical equations that include logical connectors such as, and, and not, or, nor, and the like. For example, a logical expression for automatically placing a user on an include list may be represented by the generic logical equation A or B, and C, and D. Wherein the elements A, B, C, and D may for example include A being a first user role, B being a second user role, C being a given client, and D being a given set of permissions. For example, the first user role may be billing attorney, the second user role may be working attorney, the given client may be Acme, and the given set of permissions being all available permissions. Similar logical equation can be provided for placing a user on an exclude list for the Case Data Unit level access information for a given Case Data Unit. For example, a generic equation may be L or M, and N, and not O. Wherein the elements L, M, N, and O may for example include L being a first client, M being a second client, N being a user who has worked for the first or second client and O being the role of system administrator. Thus, a user "Jane Wright" assigned to the role working attorney (not system administrator), who has worked for the first and second client L and M may be

automatically placed on an exclude list for the Case Data Unit level access information for a Case Data Unit for a client say Acme who is adverse to both L and M.

[54D] According to another embodiment of the present invention, users may be manually added to include or exclude lists for Case Data Unit level access information for given Case Data Units. Each of these embodiments provides the special needs of legal systems for limiting or granting access to cases based on ethical issues, business concerns, or other desires.

[54E] According to another embodiment of the present invention, the roles and permissions assigned to a user may be overridden by Case Data Unit level access information. The embodiment provides that if a user is placed in the include list for a Case Data Unit, the user is granted all permission related to the Case Data Unit and its associated documents.

[54E] According to an embodiment of the present invention, each Case Data Unit has an associated private folder. Private folder may contain information IP data and document related to an IP case the some users want to keep secret from other users of a Case Data Unit. Thus, while some users have access to a given private folders, other users are excluded from accessing the given private folder. Accessibility to a given private folder is controlled by group assignment. If a user and private folders assigned the same group, or if a user's group contains the private folder's group, the user will be able to perform operations upon the private folder and/or its associated documents. For example, a case having an associated Case Data Unit may be assigned to two groups, say group 1 and group 2. However, the private folder associated with the case data may only be assigned to group 1 and not assigned to group 2. Further, a user 1 may be assigned to group 1 while not being assigned to group 2. Further yet, a user 2 may be assigned to group 2 while not being assigned to group 1. Accordingly, as the private folder and user 1 are commonly assigned to group 1, user 1 will be permitted to perform operations upon the private folder and its associated documents. However, while user 2 has access to the Case Data Unit, user 2 does have access private folder because user 2 and the private folder are not assigned to the same group and user 2's group does not contain the group to which the private folder is assigned. But, if user 2 is assigned to a group, say group 3 containing group 1, then user 2 will be permitted to perform operations upon the private folder and its associated documents.

[54F] Fig. 8 is a simplified high-level flowchart 900 depicting a method of a data access technique for the data and documents of a Case Data Unit according to an embodiment of the

present invention that includes roles and permissions, groups, and Case Data Unit level access information. The method depicted in Fig. 8 may be used to either grant or deny operation requests upon the Case Data Unit and it associated documents. The processing depicted in Fig. 9 is merely illustrative of an embodiment incorporating the present invention and does not limit the scope of the invention recited in the claims. One of ordinary skill in the art would recognize other variations, modification, and alternatives.

[54G] The method is initiated by a computer receiving a request from a user to perform an operation on a Case Data Unit and/or the documents of a Case Data Unit 905. The term computer is broadly construed to include several types of computing devices including servers, computer networks, personal computers, hand held devices, or combinations of these as well as other such devices. After receiving the request a determination of the Case Data Unit level access information's include and exclude lists is made 910. Determinant upon the Case Data Unit level access information, the user may be excluded from performing the requested operation, a determination of the user's assigned roles and permission is made, or a determination of the Case Data Unit's group assignment is made 915. Case Data Unit level access information may specifically exclude a given user from performing any operations on a Case Data Unit and/or its associated documents in which case the operation request is denied 920. Alternatively, Case Data Unit level access information may specifically include the user triggering a determination of the roles and permissions assigned to the user 925. Subsequent to a determination of the roles and permissions assigned to the user 925, a determination of the particular document type the user has requested to perform an operation on is made 950. If the operation requested by the user is not one provided for in the user's assigned permission 955 the operation request is denied 960. Alternatively, if the operation requested is one permitted by the user's assigned permission upon the particular document type 955 the user's operation request is granted 965.

[54H] Alternatively, step 915 provides that Case Data Unit level access information may neither exclude nor include the user's operation request in which case a determination of the Case Data Unit's group assignment is made 930. Subsequent to the determination of the group assignment for the Case Data Unit, a determination of the user's group assignment is made 935. One of two possible steps will be taken based upon whether the user and Case Data Unit are assigned to the same group or whether the user's group includes the group to which the Case

Data Unit is assigned 940. If the user and Case Data Unit are not assigned to a the same group or if the user's group does not contain the group to which the Case Data Unit is assigned, the user is excluded from performing the requested operation on the Case Data Unit and/or documents of the Case Data Unit 945. However, if the user and Case Data Unit are assigned to the same group or if the user's group contains the Case Data Unit's group, a determination is made of the roles and permissions assigned to the user 925. Subsequent to a determination of the roles and permissions assigned to the user 925, a determination of the particular document type the user has requested to perform an operation on is made 950. If the operation requested by the user is not one provided for in the user's assigned permission 955 the operation request is denied 960. Alternatively, if the operation requested is one permitted by the user's assigned permission upon the particular document type 955 the user's operation request is granted 965.

[54I] Fig. 9 is a simplified high-level flowchart 1000 depicting a method of a data access technique for a private folder and its associated documents according to an embodiment of the present invention that includes groups. The method depicted in Fig. 9 may be used to either grant or deny operation requests upon the private folder and its associated documents. The processing depicted in Fig. 9 is merely illustrative of an embodiment incorporating the present invention and does not limit the scope of the invention recited in the claims. One of ordinary skill in the art would recognize other variations, modification, and alternatives.

[54J] The method is initiated by a computer receiving a request from a user to perform an operation on a Case Data Unit and/or it associated documents 1010. The term computer is broadly construed to include several types of computing devices including servers, computer networks, personal computers, hand held devices, or combinations of these as well as other such devices. Subsequent to the computer receiving the request, the group assignments of the private folder is determined 1020 and the group assignment of the user is determined 1030. One of two possible steps will be taken based upon whether the user and private folder are assigned to the same group or whether the user's group contains the group to which the private folder is assigned 1035. One of the steps is to deny the operation requested upon the private folder and/or its associated documents if the user and private folder are not assigned to the same group or if the user's group does not contain the group to which the private folder is assigned 1040. The other step is to allow the user to perform the operation on the private folder and/or its documents if the

user and the private folder are assigned to the same group or the user's group contains the group to which the Case Data Unit is assigned 1045.

[54K] Further details of the use of roles, permissions, groups, private folders and Case Data Units according to one embodiment of the invention are set forth in concurrently filed U.S. Provisional Application Number 60/333,962 entitled "DATA ACCESS CONTROL TECHNIQUES USING ROLES AND PERMISSIONS" and having Stephen K. Boyer, Jeffry J. Grainger and Cecily Anne Snyder as inventors. The 60/333,962 application is hereby incorporated by reference in its entirety.